IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	RAIKAR, et al.	Patent Application	
Application No.:	10/632,446	Group Art Unit:	2143
Filed:	July 31, 2003	Examiner:	Shin, Kyung H.

For: CONFIGURING SECURE TEMPLATES FOR AN APPLICATION AND NETWORK MANAGEMENT SYSTEM

REPLY BRIEF

In response to the Examiner's Answer mailed on June 13, 2008, Appellants respectfully submit the following remarks.

REMARKS

Appellants are submitting the following remarks in response to the Examiner's Answer. In these remarks, Appellants are addressing certain arguments presented in the Examiner's Answer. While only certain arguments are addressed in this Reply Brief, this should not be construed that Appellants agree with the other arguments presented in the Examiner's Answer.

DESAI

This section describes Appellants understanding of what Desai teaches. Desai teaches combining log-based and knowledge-based systems (paragraph 0106). At the second sentence of paragraph 0108 Desai states, "...log-based systems see all traffic traversing the network, including traffic that is dropped at the firewall" (emphasis added). At paragraph 0110, Desai states, "...knowledge-based systems apply the signature knowledge accumulated about specific attacks and system vulnerabilities to detect intrusions" (emphasis added). Desai mentions "templates" paragraphs 0022, 0023, and 0101. Since these are the only three locations that Desai mentions "templates," Appellants are uncertain which of Desai's filtering processes teach Desai's templates. Desai's sensors appear to be a part of Desai's knowledge based system.

Referring to paragraph 0039, Desai appears to combine a log-based and knowledge based system by using a network/host based intrusion detection system, a log-based event classification system, and interactions and correlations between them. Desai discusses the log-based event classification system from paragraph 0040 to paragraph 0085. Desai discusses the network/host based intrusion detection system starting at paragraph 0086. Appellants are unsure exactly where Desai begins to discuss the correlation between the network/host based intrusion detection

system and the log-based event classification system, however, it appears that Desai begins one discussion of the correlation at paragraph 0100 but also mixes the discussion of the correlation in with Desai's discussion of the network/host based intrusion detection system and the log-based event classification system.

Desai discusses filtering types of processing as a part of his log-based event classification system, his network/host based intrusion detection system, and his correlation. For example, the log-based event classification filtering type processing appears to be described from paragraphs 0055-0062. The network/host based intrusion detection filtering type processing appears to be described from paragraphs 0089-0095. Desai discusses the correlation filtering type processing from paragraph 0101 on. However, the description of the correlation filtering type processing also appears to be mixed in with the log-based event classification description and the network/host based intrusion detection system. For example, at paragraph 0100 Desai states, "FIG. 4 is a schematic diagram of an exemplary hardware configuration for a combined and correlated log based event classification system and network-based intrusion detection and response system. Fig. 4 depicts log-event collector(s) 20, event analysis engine 30 and event correlation engine 40. For example, the log-event collector(s) 20 are described at 0045-0048, 0095-0096. The event analysis engine 30 is described at 0049-0054, 0056-0077 and 0096-0098. The event correlation engine 40 is described at paragraph 0079-0083.

Desai's log-based event classification system, Desai's network/hosted based intrusion detection system, and Desai's combined correlation log based event classification system analyzes detected information.

With regards to Desai's log-based event classification filtering processing, Desai' states starting at line 5 of paragraph 0055 "It is important to strike a balance in logging, ensuring that the 'right things' are being logged as opposed to logging 'everything.'" Desai's log-based event classification filtering process determines whether to create a log based on detected information. A copy of the log is eventually transmitted to the centralized management center (0063). Appellants understand the event analysis engine 30 to be a part of the centralized management center (0065) since paragraph 0101 states that FIG. 4 depicts "a combined and correlated …system" and the event analysis engine 30 is depicted in Figures 4 and 5.

Desai's log-based event classification filtering processing referred to in paragraph 0055 appears to occur before Desai's "secure central log/event collector 20" since Desai's secure central log/event collector 20 receives created logs (paragraph 0043). Therefore, it appears that Desai's log-based event classification filtering processing referred to in paragraph 0055 determines whether to create logs. The created logs are transmitted to the central log/event collector 20 and are eventually processed by the event analysis engine 30 and the event correlation engine 40.

With regards to Desai's network/host based intrusion detection filtering process, Desai appears to use sensors that "sniff" the wire and compare live traffic patterns to a list of known attack patterns (paragraph 0091). The "…sensors can be configured to automatically respond to intrusion attempts before they have a chance to do any damage. Responses might include: (i)

kill or reset malicious TCP connections; (ii) block offending IP address's on firewalls; or (iii) execute any user-defined programs or batch files."

Desai's log-based event classification system (0063-0083) and network/host based intrusion detection system (0095) transmit copies of logs to Desai's combined correlation system.

With regards to Desai's combined correlation filtering processing, Desai states in the second sentence of paragraph 0101, "Using pre-defined templates the central security management team can more quickly identify new or changing vulnerability trends."

THE DIFFERENCE BETWEEN DESAI AND THE RECITED EMBODIMENTS.

This section describes why Appellants believe that the embodiments recited by the claims are not anticipated by Desai. Appellants were able to find three places that Desai mentions "templates." For example, Desai states in paragraph 0022, "log-based abnormal behavior by employing pre-defined templates based upon on the type profile of an enterprise" and in paragraph 0023 "knowledge-based attack signatures by employing pre-defined templates based upon on the type/profile of an enterprise." Desai also describes various filtering processes in various places. However, Appellants do not understand Desai to clearly disclose what processes are used to as a part of Desai's "templates." Despite this deficiency, Appellants will demonstrate why various filtering processes of Desai do not teach the recited embodiments.

As a part of asserting that Desai anticipates Claim 1, the Examiner's Answer relies on filtering processes that are scattered through out Desai's system. Claim 1 recites, "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template; configuring the template with second information for processing the data associated with at least one of the received messages; and configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system" (emphasis added).

For example, the Examiner's Answer relies on filtering processes described in paragraph 0055 and 0091 to teach "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template." However, 0055 discloses filtering processes that are a part of Desai's log-based event classification system and 0089 discloses filtering processes that are a part of Desai's network/host based intrusion detection system.

In another example, the Examiner's Answer relies on paragraph 0049 and paragraph 0053 to teach "configuring the template with second information for processing the data associated with at least one of the received messages." Although paragraph 0049 appears in the log-based event classification system, since paragraph 0049 refers the Event Analysis Engine 30, which appears to be a part of the combined correlation system, for reasons provided herein.

Paragraph 0053 refers to de-duplicating and comparing events after data is collected and therefore appears to be referring to the event analysis engine 30. Therefore, the Examiner's Answer relies on filter processing that occurs before Desai's central log/event collector 20 (0043, 0055), filter processing provided by "agents" and "sensors" as a part of Network/Host Based Intrusion Detection System, and filter processing provided by (0089), and filter processing provided by the combined correlation system (0049) to teach "configuring a template...with first information…configuring the template with second information… configuring the template with third information…," as recited by Claim 1 where a single template is configured with first information, second information and third information.

Referring to paragraph 0055 lines 1-14, assume that either Desai's "created logs" or the real-time information that Desai's log-based event classification filtering process teaches the "data" referred to in "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template," (emphasis added) recited by Claim 1.

In the first case of Desai's created logs teaching Claim 1's data, Appellants do not understand Desai's log-based event classification filtering process to determine whether Desai's created logs associated with at least one message received by Desai's log-based event classification filtering process should or should not be processed by Desai's log-based event classification filtering process. Instead, Appellants understand Desai to teach that Desai's log-based event classification filtering process determines whether to create a log. The copy of the

log is eventually transmitted to Desai's Event Analysis Engine 30 (0063 and 0065), which Appellants understand to be a part of Desai's centralized management center (paragraph 0063).

In the second case of Desai's real-time information teaching Claim 1's data and Desai's "creating a log" to teach Claim 1's "processed by the template," Appellants understand Desai's log-based event classification filtering process to always process Desai's real-time information in order to determine whether to create a log. Desai would not be able to determine whether to create a log for a received piece of real-time information if Desai did not process that received piece of real-time information. Therefore, Appellants do not understand Desai's real-time information to teach the data referred to in "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template," (emphasis added) as recited by Claim 1.

The Examiner's Answer states at page 13 lines 5-12, "Desai discloses a determination to process event messages concerning a particular event or not to process the event messages...(Desai paragraph 0089, || 7-11..." Desai states at lines 7-11 of paragraph 0089,

> Host-based agents can be configured to automatically respond to intrusion attempts before they have a chance to do any damage. Responses might include: (i) kill or reset malicious TCP connections; or (ii) execute any user-defined programs or batch files (emphasis added).

First, Desai states that an automatic response is made which does not qualify as "determining whether data associated with at least one message received by the template should or should not be processed." Further, "an automatic response is made" (emphasis added) teaches

away from "determining whether data…should not be processed." Appellants respectfully point out that Desai in lines 7-9 of paragraph 0089 goes on to give examples of an automatic response by stating "Responses might include: (i) kill or reset malicious TCP connections; or (ii) execute any user-defined programs or batch files." Appellants respectfully submit that killing or resetting malicious TCP connections or executing any user-defined programs or batch files does not teach "determining whether data…should or should not be processed…" Appellants understand killing or resetting malicious TCP connections or executing any user-defined programs or batch files to teach away from "determining whether data…should or should not be processed…"

The Examiner's Answer states with regards to the response to A.2 at lines 19-20, "Desai discloses processing an event message and associated data based on the template." The Examiner's Answer refers to paragraph 0049 lines 1-7 and paragraph 0053 lines 1-7. It appears that paragraph 0053 describes processing that occurs before the "secure central log/event collector 20" receives "copies of the log events" (0043). The discussion of Desai's event analysis engine 30, which is a part of Desai's combined correlation log based event classification system, starts at paragraph 0049 and proceeds passed paragraph 0053. Therefore, the filter processing referred to by the Examiner's Answer for A.2 resides in two different parts of Desai's system. Therefore, Appellants respectfully submit that paragraph 0049 lines 1-7 and paragraph 0053 line 1-7 do not teach "configuring a template…configuring the template… configuring the template…," as recited by Claim 1 for at least the reason that Desai's filtering process is scattered around Desai's system.

The Examiner's Answer states with regards to the response to A.3 at lines 14-16, "there is no disclosure that all event messages are processed based on the fact that logfile data is processed. Desai also disclose that real-time data is processed."

The Examiner's Answer does not specify a portion of Desai that it is replying on. First, even if Desai teaches filtering of real time data, Desai's filtering process is scattered around Desai's system. For at least this reason Desai does not teach "configuring a template...configuring the template... configuring the template...," as recited by Claim 1.

Second, even if Desai' teaches filtering real time data, this is not evidence that Desai' teaches "configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system," (emphasis added) as recited by Claim 1.

Third, since the Examiner's Answer refers to "real-time data" in the response to A.3, it appears that the Examiner's Answer is referring to either paragraph 0055, which describes filtering process that occurs before Desai's "secure central log/event collect 20" (0043), or paragraph 0091, which describes Desai's sensors. The Examiner's Answer also relied on paragraph 0055 and 0091 to teach "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template," as recited by Claim 1. Paragraphs 0055 and 0091 cannot teach both "configuring a template for an application and network management system with first information for determining whether data

associated with at least one message received by the template should or should not be processed by the template," as recited by Claim 1" (emphasis added) and teach "configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system," (emphasis added) as recited by Claim 1. Therefore, the Examiner's Answer seems to assert that Desai's so called "first information" and "third information" are the same. In this case, Desai would not teach "configuring a template with first information…configuring the template with third information" because Claim 1 recites that "first information" is for "determining whether data associated with at least one message received by the template should or should not be processed" and "third information" is for "preventing the communication of at least one received message to other templates…"

The Examiner's Answer states in the first sentence of page 15, "Appellant seems to base his assertion that all data is processed (Appeal Remarks Page 17) or the fact that Desai mentions logfile type data as one type of information processed." At page 15 lines 6-9, the Examiner's Answer states, "Desai disclose that not all data is processed as logfile data. (Desai paragraph 055, lines 1-14; selective information is processed; increasing or decreasing logging information for different types of services (event processing and other types of traffic)." First, Appellants respectfully submit that Desai does not clearly indicate that the processing described in paragraph 055 lines 1-14 are a part of one of Desai's templates. Further, Desai's so called filter processing is scattered around Desai's system. Therefore, for at least these reasons, Appellants respectfully submit that Desai does not teach "configuring a template…configuring the template… configuring the template…," as recited by Claim 1.

Appellants believe that Appellants' responses provided above and provided in the Appeal Brief address the rest of the Examiner's Answer. Therefore, Appellants will not continue responding to the rest of the Examiner's Answer.

SUMMARY

For at least the reason that Desai's filter processing is scattered around Desai's system, Appellants respectfully submit that Desai does not anticipate the embodiment recited by Claim 1 which recites that "configuring a template...with first information…configuring the template with second information… configuring the template with third information…"

For reasons provided herein, Appellants respectfully submit that neither Desai's copies of logs nor Desai's real-time information described at paragraph 0055 lines 1-14 teach "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template," as recited by Claim 1.

For at least the reasons that paragraph 0089 lines 7-11 discloses that an automatic response teaches away from "determining whether data…should not be processed," as recited by Claim 1, Applicants respectfully submit that Desai does not anticipate "determining whether data…should not be processed."

Lastly, since the Examiner's Answer relies on the same portions of Desai (0055 and 0091) to teach Claim 1's "first information" and "third information," Appellants do not understand Desai to teach "configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system," as recited by Claim 1.

For at least these reasons, independent Claim 1 should be patentable. For similar reasons independent Claims 8 and 14 should also be patentable. Claims 2-7 depend on Claim 1 in that Claim 8 and 14 respectively recite "receiving first information entered by a developer to configure a template of an application and network management system for determining whether data associated with at least one message received by the template should or should not be processed by the template; receiving second information entered by the developer to configure the template to process the data associated with at least one of the received messages; and receiving third information entered by the developer to configure the template to prevent the communication of at least one received message to other templates of the application and network management system" and "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template; configuring the template with second information for processing the data associated with at least one of the received messages; and configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system."

Claims 9-13 depend on Claim 8. Claims 15-19 depend on Claim 14. These dependent claims include all of the features of their respective independent claims. Further, these dependent claims include additional features which further make them patentable. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable.

In summary, Appellants respectfully submit that the Office Action's rejections of the claims are improper as the rejection of Claims 1-7 and 14-19 does not satisfy the requirements of a prima facie case of anticipation. Accordingly, Appellants respectfully submit that the rejection of Claims 1-7 and 14-19 under 35 U.S.C. §102(e) are improper and should be reversed.

CONCLUSION

In view of the above remarks, Appellants continue to assert that Desai does not teach the claimed embodiments, for reasons presented above and for reasons previously presented in the Appeal Brief.

Respectfully submitted,

WAGNER BLECHER LLP

Dated: 08/04/2008

/John P. Wagner, Jr./
John P. Wagner, Jr.
Registration Number: 35,398

WAGNER BLECHER LLP
123 Westridge Drive
Watsonville, CA 95076
(408) 377-0500